

Amendments to the Specification

Please replace the paragraph that begins on Page 21, line 14 and carries over to Page 22, line 3 with the following marked-up replacement paragraph:

-- Returning again to the discussion of Fig. 4, following the authentication performed at Block 430, the authentication service publishes the generated assertion (Block 440) to the local trust proxy. (That is, if the authentication was successful, this assertion indicates that the user is authentic.) See message flow 505. Upon receiving this assertion, the local trust proxy preferably validates the authenticator's digital signature and if valid, routes the assertion in a message to a peer trust proxy in one or more of the remote security domains (Block 450). See message flow 506. As discussed above with reference to Block 420, this routing at Block 450 preferably uses policy to determine the authorized recipients. In the example, the authorized recipient is remote trust proxy ~~[[251]]~~ 231. --

Please replace the paragraph on Page 22, lines 4 - 9 with the following marked-up replacement paragraph:

-- In addition to routing the assertion to the remote security domain, as shown by message flow 506, the trust proxy ~~[[252]]~~ 232 preferably also returns each authentication response generated by an authentication service within the federation (such as the response published at Block 440) to the point-of-contact service (which in this case is the distributed portal 210). This has not been illustrated in Fig. 5. (The point-of-contact service preferably uses the authentication responses from the various other services when aggregating the view to be presented to the user.) --

Please replace the paragraph on Page 22, lines 10 - 20 with the following marked-up replacement paragraph:

-- Upon receiving the message sent from the local trust proxy at Block 450, the remote trust proxy applies what is referred to herein as “credential mapping”, whereby the identifying information in the message is mapped to a locally-managed identity (Block 460). Suppose, for example, that while Sally is authenticated to the local security domain using the user ID “sally@cedar.net” and corresponding password “federate”, her user ID and password as an employee of SFS are “spjenkins@sfs.com” and “investments-R-Us”. Accordingly, the processing at Block 460 comprises determining that the authentication assertion received from the local trust proxy is, in fact, an authentication of this same user. This credential mapping operation is shown as activity 507 in Fig. 5. (Trust proxy [[251]] 231 may invoke a separate service within remote security domain 200 when performing this credential mapping, without deviating from the scope of the present invention, although this has not been shown in Fig. 5.) --

Please replace the paragraph on Page 23, lines 8 - 15 with the following marked-up replacement paragraph:

-- Fig. 7 depicts a sample response message 700 conveying authentication results for the example scenario. As shown therein, SOAP message body 740 indicates (at reference number 741) that this is a multi-domain authentication response, created within the security domain referred to as “domain2A”, where the result of the authentication is “permit” (see reference number 742). This result indicates that the user to whom the user name 731 and password 732 credentials of UsernameToken [[740]] 730 correspond is permitted to access the requested

remote portlet 240. Reference number 720 indicates that the signer of this authentication response message is “securityGateway2A”, which in the example represents authentication service 251. --

Please replace the paragraph that begins on Page 24, line 8 and carries over to Page 25, line 7 with the following marked-up replacement paragraph:

-- Commonly-assigned and co-pending U. S. Patent Application 20030135628 (serial number 10/047,811; attorney docket ~~RSW920030199US1~~ RSW920010199US1), which is titled “Provisioning Aggregated Services in a Distributed Computing Environment”, discloses techniques that enable heterogeneous identity systems to be joined in the dynamic, run-time Web services integration environment. This application, referred to herein as “the provisioning invention”, is hereby incorporated herein by reference. A provisioning interface was disclosed in the provisioning invention to enable automatically and dynamically federating the heterogeneous identity systems which may be in use among the services which are aggregated as a composite service. The techniques disclosed therein allow users (whether human or programmatic) to be seamlessly authenticated and authorized, or “identified”, for using the dynamically-integrated services. According to the provisioning invention, this seamless identification may be provided using a single sign-on, or “unified login”, for an aggregated service, wherein the provisioning interface of the aggregated service can be used to solicit all required information from a user at the outset of executing the aggregated service. A “stacking” approach was described whereby user passwords (or other credentials, equivalently, such as tickets or digital certificates) to be provided to the sub-services of an aggregated service are encrypted for securely storing. The sub-

services are invoked in a specified order during execution, according to a definition that is preferably specified in the Web Services Flow Language (“WSFL”), and the stacked passwords are then unstacked and presented to the appropriate authentication or authorization sub-service. -